PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-288940
(43)Date of publication of application : 01.11.1996

(51)Int.Cl. H04L 9/08
G06F 15/00
G09C 1/00
H04H 1/00
H04N 7/167

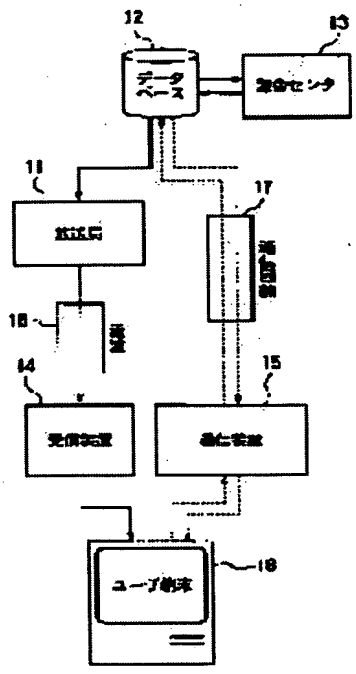
(21)Application number : 07-346095
(22)Date of filing : 11.12.1995

(71)Applicant : MITSUBISHI CORP
(72)Inventor : SAITO MAKOTO
MOMIKI JIYUNICHI

(30)Priority
Priority number : 06309292 Priority date : 13.12.1994 Priority country : JP

(54) CIPHERING KEY SYSTEM

(57)Abstract:
PURPOSE: To prevent illicit use by using a secret key so as to cipher data, sending the data to a data communication equipment via a communication channel and decoding the received data through the use of the secret key.
CONSTITUTION: A data communication equipment 15 is used to apply the use of data to a database 12 via a communication channel 17. In this case, the user ciphers his own secret key by using an open key of the database 12 and sends the cryptographic key to the database 12. The database 12 decodes the ciphered secret key of the user by using an exclusive key, ciphers the data applied for the use by using the secret key of the user to be decoded and sends the ciphered data to the equipment 15 via the channel 17. The user receiving the data ciphered by using his own secret key uses a user terminal equipment 18 to decode the ciphered data ciphered by using his own secret key. Moreover, a charge center 13 is provided to the database 12 to be used for account of the charge attending intake/issue of orders.



LEGAL STATUS
[Date of request for examination] 18.10.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or

REF. 88674
CITED IN JP
REJ. DTD

application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－288940

(43)公開日　平成８年(1996)11月１日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/08		8842－5Ｊ	Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｇ０６Ｆ　15/00	３３０	9364－5Ｌ	Ｇ０６Ｆ　15/00	３３０Ｚ	
Ｇ０９Ｃ　1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６３０Ｆ	
		7259－5Ｊ		６３０Ｂ	
Ｈ０４Ｈ　1/00			Ｈ０４Ｈ　1/00	Ｆ	

審査請求　未請求　請求項の数８　ＦＤ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平7－346095

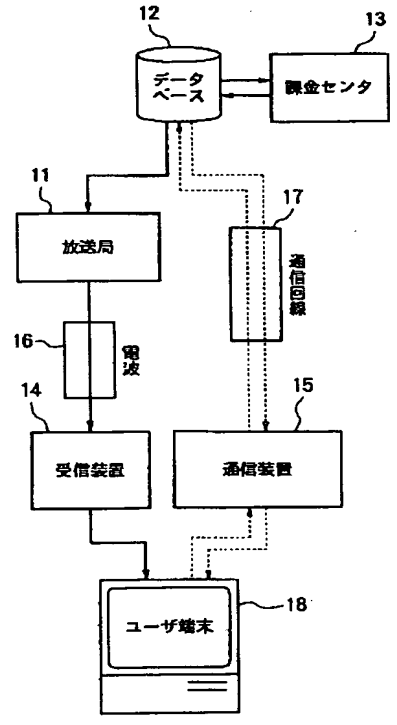
(22)出願日　平成７年(1995)12月11日

(31)優先権主張番号　特願平6－309292
(32)優先日　平６(1994)12月13日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005979
三菱商事株式会社
東京都千代田区丸の内２丁目６番３号
(72)発明者　斉藤　誠
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内
(72)発明者　粉木　隼一
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内
(74)代理人　弁理士　南條　眞一郎

(54)【発明の名称】　暗号鍵システム

(57)【要約】
【課題】　暗号鍵システムの発明をテレビジョンシステム、データベースシステムあるいは電子商取引システム等に適用するための具体的な構成を得る。
【解決手段】　このシステムは放送局、データベース、受信装置、データ通信装置及びユーザ端末装置から構成され、暗号鍵方式としては秘密鍵方式、公開鍵方式、デジタル署名方式が用いられこれらの鍵は暗号化されあるいは暗号化されないで放送によって供給される。本発明は、データベースシステムの不正利用の防止、著作権の管理、ペイパービューシステム、ビデオオンデマンドシステムにおいて有効であり、さらには電子データ情報システムを利用した電子マーケットの実現において有効な手段である。



【特許請求の範囲】
【請求項１】　放送局、データベース、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって：前記暗号鍵システムは、
前記データベースと前記放送局との間は専用回線等のオンライン通信手段あるいはフレキシブルディスク等のオフライン手段で接続され；前記データベースと前記データ通信装置の間は通信回線で接続され；前記放送局と前記受信装置の間は電波で接続され；前記受信装置と前記ユーザ端末装置との間及び前記データ通信装置と前記ユーザ端末装置との間は直接にオンライン手段であるいはフレキシブルディスク等のオフライン手段で接続され；前記データベースは公開鍵と専用鍵を用意して前記放送局に前記公開鍵を供給し；前記放送局は受け取った前記公開鍵を放送し；前記受信装置は受信した前記公開鍵を前記ユーザ端末装置に転送し；前記ユーザ端末装置は転送された前記公開鍵を保存し；ユーザは希望するデータの利用を申し込む際にユーザの秘密鍵を前記受信した公開鍵を用いて暗号化して前記データベースに送信し；データの利用申込を受けた前記データベースは、前記ユーザの前記秘密鍵を前記専用鍵を用いて復号化し、復号された前記ユーザの前記秘密鍵を用いてデータを暗号化し、前記通信回線を経由して前記データ通信装置に送信し；前記ユーザは受け取ったデータを前記ユーザ端末装置に転送し、前記秘密鍵を用いてデータを復号化する暗号鍵システム。
【請求項２】　前記公開鍵に前記データベースのデジタル署名がなされているクレーム１の暗号鍵システム。
【請求項３】　ＣＡＴＶ放送局、課金センタ、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって：前記暗号鍵システムは、
前記ＣＡＴＶ放送局と前記受信装置の間及び前記ＣＡＴＶ放送局と前記データ通信装置の間はＣＡＴＶ回線で接続され；前記受信装置と前記ユーザ端末装置との間及び前記データ通信装置と前記ユーザ端末装置との間は直接にオンライン手段によってあるいはフレキシブルディスク等のオフライン手段で接続され；ユーザはユーザの公開鍵をＣＡＴＶ放送局に予め登録するか又は利用申込時に提示し；前記ＣＡＴＶ放送局はテレビジョン番組をＣＡＴＶ放送局の前記秘密鍵を用いて暗号化し、利用申込を行った前記ユーザの公開鍵を用いて前記ＣＡＴＶ放送局の利用許可鍵である秘密鍵を暗号化してＣＡＴＶ回線を経由して放送し；前記ユーザは前記受信装置で前記テレビジョン番組及び前記秘密鍵を受信し、前記公開鍵に対応する専用鍵を用いて前記秘密鍵を復号化し、復号された前記秘密鍵でテレビジョン番組を復号化する暗号鍵システム。
【請求項４】　ＣＡＴＶ放送局、データ管理センタ、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって：前記暗号鍵システムは、
前記ＣＡＴＶ放送局と前記データ管理センタの間は専用回線等のオンライン通信手段あるいはフレキシブルディスク等のオフライン手段で接続され；前記ＣＡＴＶ放送局と前記受信装置の間及び前記ＣＡＴＶ放送局と前記データ通信装置の間はＣＡＴＶ回線で接続され；前記受信装置と前記ユーザ端末装置との間及び前記データ通信装置と前記ユーザ端末装置との間は直接にオンライン手段であるいはフレキシブルディスク等のオフライン手段で接続され；前記データ管理センタは公開鍵と供給するデータ各々の秘密鍵を用意し前記ＣＡＴＶ放送局に供給し；前記ＣＡＴＶ放送局は前記データ管理センタの公開鍵を用いて前記データ管理センタの秘密鍵を暗号化して放送し；ユーザは前記データ通信装置を用いて前記ＣＡＴＶ回線を経由し前記ＣＡＴＶ放送局を介して前記データ管理センタにデータの利用を申し込むとともに前記ユーザの公開鍵を送信し；前記データ管理センタは前記データ各々の秘密鍵を用いて各々のデータを暗号化し、前記ユーザの公開鍵を用いて前記データ管理センタの公開鍵を暗号化し、暗号化された各々のデータ、暗号化された前記データ管理センタの公開鍵及びデータ管理センタの専用鍵を前記ユーザに送信し；前記ユーザは前記ユーザの専用鍵を用いて前記データ管理センタの公開鍵を復号化し、復号化された前記データ管理センタの公開鍵を用いて暗号化された前記データ各々の秘密鍵を復号化し、複合化された前記データ各々の秘密鍵を用いて前記各々のデータを復号化する暗号鍵システム。
【請求項５】　前記公開鍵に前記データ管理センタのデジタル署名がなされているクレーム４の暗号鍵システム。
【請求項６】　ＣＡＴＶ放送局、データ管理センタ、受信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって：前記暗号鍵システムは、
ユーザの公開鍵を予め前記データ管理センタに登録しておき；前記データ管理センタは、前記データ管理センタの公開鍵を前記各ユーザの公開鍵を用いて暗号化し、前記データ管理センタの専用鍵を用いて前記データ管理センタの公開鍵にデジタル署名を行い；暗号化された前記データ管理センタの公開鍵及び前記データ管理センタのデジタル署名をＣＡＴＶ放送局に送信し；前記ＣＡＴＶ放送局は暗号化された前記データ管理センタの公開鍵及びデジタル署名を放送し；前記ユーザは前記ユーザの公開鍵を用いて受信した前記データ管理センタの暗号化公開鍵を復号化するとともに前記復号化されたデータ管理センタの公開鍵を用いてデジタル署名を確認する暗号鍵システム。
【請求項７】　さらに、各ユーザの暗号化されていないユーザ識別情報が暗号化された前記データ管理センタの公開鍵に付与して放送されるクレーム６の暗号鍵システム。
【請求項８】　ＣＡＴＶ放送局、データ管理センタ、受

信装置、データ通信装置及びユーザ端末装置から構成される暗号鍵システムであって：前記暗号鍵システムは、ユーザは前記データ管理センタにデータの利用を要求する毎に前記ユーザの公開鍵を前記データ管理センタに提示し；前記ユーザからのデータ利用要求を受けた前記データ管理センタは利用要求されたデータを前記ユーザの公開鍵を用いて暗号化して前記ＣＡＴＶ放送局に送信し；前記ＣＡＴＶ放送局は受け取った前記暗号化されたデータを放送し；放送された前記暗号化データを受信した前記ユーザは前記暗号化データを前記ユーザの専用鍵を用いて復号化する暗号鍵システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、テレビジョンシステム、データベースシステムあるいは電子情報交換（Electronic Data Interchange：ＥＤＩ）を利用する商取引システム等において用いられる暗号鍵システムに係るものである。

【０００２】

【従来の技術】情報化時代と言われる今日、通常の地上波放送の他に放送衛星（ＢＳ）、通信衛星（ＣＳ）と呼ばれる衛星放送、同軸ケーブルあるいは光ケーブルを利用したＣＡＴＶと呼ばれる有線ＴＶ放送が普及しつつある。

【０００３】同時に数１０チャンネルを配信することができる衛星放送あるいはＣＡＴＶ放送においては、包括的な契約によって視聴することができるスクランブルがかけられていない一般的なチャンネルの他に、包括的な契約によっては視聴することができないスクランブルされた映画・スポーツ・音楽等専門的なチャンネルが設けられている。これらのチャンネルを視聴するためにはスクランブルを解除するするために契約を行う必要があるが、この契約期間は通常１カ月程度の単位で行われるため、随時の契約によって視聴することができない。

【０００４】本発明者らは、特開平６－４６４１９号及び特開平６－１４１０００４号で公衆電信電話回線を通じて課金センタから視聴許可鍵を入手するとともに課金が行われ、視聴許可鍵を用いて番組毎に異なるスクランブルパターンで行われたスクランブルを解除して番組を視聴するシステムを、特開平６－１３２９１６号でそのための装置を提案した。

【０００５】これらのシステム及び装置において、スクランブルされた番組利用希望者は通信装置を使用し通信回線を経由して課金センタに利用申し込みを行い、課金センタはこの利用申し込みに対して通信装置に許可鍵を送信するとともに課金処理を行い料金を徴収する。通信装置で許可鍵を受信した利用希望者は通信装置と受信装置を接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって番組のスクランブルを解除し、利用希望者が番組を利用する。

【０００６】特開平６－１３２９１６号にはこれらのシステム及び装置の応用として、各々異なるスクランブルパターンでスクランブルされた複数のデータが記録されたテープあるいはディスクを販売あるいは貸与し、ＩＣカード等により利用許可鍵を供給して特定のデータを利用するシステム及び装置も記載されている。

【０００７】また、情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータをＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）、これらを相互に接続したインターネットシステムによってコンピュータ通信ネットワークを構成し、相互に利用するデータベースシステムが普及しつつある。

【０００８】一方、デジタル化すると情報量が膨大になるためデジタル化することができなかったテレビジョン動画信号を、圧縮することにより情報量を減少させ、実用的なデジタル化を可能にする技術が開発され、これまでにテレビジョン会議用のＨ．２６１規格，静止画像用のＪＰＥＧ（Joint Photographic image coding Experts Group）規格，画像蓄積用のＭＰＥＧ１（Moving Picture image coding Experts Group 1）規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するＭＰＥＧ２規格が作成された。

【０００９】これらの画像圧縮技術を利用したデジタル化技術はテレビジョン放送あるいはビデオ画像記録用に用いられるだけではなく、コンピュータでこれまで扱うことができなかったテレビジョン動画データを扱うことができるようになり、コンピュータが扱う各種のデータとデジタル化されたテレビジョン動画データを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。このマルチメディアシステムもデータ通信に組み入れられ、データベース上のデータの一つとして利用される。

【００１０】このようにしてデータベースの利用範囲が拡大する中で、データベース上のデータ利用に対する課金をどのようにして行うかということ及びデータの直接的な利用以外の複写あるいは転送等によって発生する著作権の問題及びデータの加工によって発生する２次的著作権の問題をどのようにして処理するかということが大きな問題となる。課金及び著作権の処理を確実に行うには、正規の利用者でなければデータの利用が不可能であるようにする必要があり、データを暗号化しておくことがそのための最良の手段である。

【００１１】また、これまで紙に記載して行ってきた各種取引における情報を電子データ化し、データ通信技術を利用して相互に送受信する電子情報交換（ＥＤＩ）を利用して電子商取引を行う電子マーケットシステムが検討されており、さらに進んで電子商取引システムの決済

を電子決済で行うことも検討されている。商取引においては取引内容の信頼性が要求され、決済においては安全性が要求される。したがって、このような信頼性と安全性が要求される電子商取引システム及び電子決済システムにおいては、データの改竄あるいは盗用が行われないようにデータを暗号化する必要がある。

【００１２】これらのテレビジョンシステム、データベースシステムあるいは電子商取引システム等において、データを暗号化し、暗号化されたデータを復号化して利用するためには暗号鍵が必要であり、データ利用者に対して暗号鍵を渡さなければならないが、この作業は安全性及び確実性が要求されるため非常に煩雑である。

【００１３】本発明はその構成においてデータ暗号技術が重要な役割を果たすが、初めにデータ暗号技術について一般的な説明を行う。データ暗号技術においては、平文データＭを暗号鍵Ｋを用いて暗号化し暗号文データＣを得る場合を

Ｃ＝Ｅ（Ｋ，Ｍ）

と表現し、暗号文データＣを暗号鍵Ｋを用いて復号化し平文データＭを得る場合を

Ｍ＝Ｄ（Ｋ，Ｃ）

と表現する。

【００１４】データ暗号化技術において用いられる代表的な方式として、秘密鍵暗号方式と、公開鍵暗号方式がある。秘密鍵方式は、暗号化と復号化に同じ秘密鍵Ｋｓを使用する暗号方式である。

Ｃmks＝Ｅ（Ｋs，Ｍ）

Ｍ＝Ｄ（Ｋs，Ｃmks）

【００１５】公開鍵方式は、暗号鍵として暗号化用の鍵と復号化用の鍵が使用され、暗号化用の鍵が公開されており、復号化用の鍵が公開されていない暗号鍵方式であり、暗号化用の鍵は公開鍵Ｋbと呼ばれ、復号化用の鍵は専用鍵Ｋvと呼ばれる。この暗号方式を使用するには、情報を送る側は平文データＭをデータを受ける側の公開鍵Ｋbを用いて暗号化し、

Ｃmkb＝Ｅ（Ｋb，Ｍ）

データを受け取った側は専用鍵Ｋvを用いて復号化し、平文データＭを得る。

Ｍ＝Ｄ（Ｋv，Ｃmkb）

この公開鍵方式は、暗号の解読が非常に困難である。

【００１６】データ暗号技術の応用として、データの信頼性を確保するために電子データ認証手段としてデジタル署名が行われることがある。デジタル署名には、秘密鍵を用いるものと公開鍵を用いるものがあるが、一般的には公開鍵を用いて署名が行われる。公開鍵を用いて行われるデジタル署名において、署名者は文書Ｍをハッシュ(Hash)アルゴリズムで圧縮した文書ｍを署名者の専用鍵Ｋvを用いて暗号化することによりデジタル署名を得、

Ｓmkv＝Ｅ（Ｋv，ｍ）

原文書Ｍあるいは圧縮文書ｍとデジタル署名Ｓmkvとを受信者に送信する。受信者は署名者の公開鍵Ｋbを用いてデジタル署名Ｓmkvを復号化し、

ｍ’＝Ｄ（Ｋb，Ｓmkv）

ｍ’＝ｍであれば、署名が正しいことが確認される。

【００１７】これらの暗号鍵を利用者に渡す方法として本発明者らは先願である特願平６－７０６４３号において「暗号鍵システム」と題する発明を提案した。一般的に行われている暗号鍵システムにおいて暗号鍵が利用者だけに渡されるのに対して、この先願発明の暗号鍵システムにおける暗号鍵は利用者以外にも渡される。

【００１８】図１に示されたのは特願平６－７０６４３号で提案された暗号鍵システムの構成である。このシステムは、ＢＳ・ＣＳ・地上波テレビジョンあるいはＦＭ等多重化放送あるいはデータ放送を行う放送局１、データベース２、課金センタ３、受信装置４、データ通信装置５及びユーザ端末装置８から構成されている。放送局１とデータベース２の間及びデータベース２と課金センタ３の間は専用回線等の通信回線あるいはフレキシブルディスク等の手段により接続されている。データベース２とデータ通信装置５の間は公衆回線あるいはＣＡＴＶ回線等の通信回線７で接続されている。放送局１と受信装置４の間は放送電波６で接続されている。受信装置４とユーザ端末装置８との間及びデータ通信装置５とユーザ端末装置８との間は接続ケーブル等の直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。なお、この図において実線で示されたのは暗号化されていない情報の経路であり、破線で示されたのは暗号化されたデータの経路である。

【００１９】このシステムにおいて、データベース２はデータ毎に異なる暗号鍵Ｋdを含む利用許可鍵Ｋp（以下「許可鍵」という）を放送局１に予め供給する。なお、理解しやすくするために、許可鍵Ｋpは暗号鍵Ｋdだけから構成されているものとして説明する。暗号鍵Ｋdは暗号化されずに供給される場合と共通暗号鍵Ｋ0を用いて暗号化され、

Ｃkdk0＝Ｅ（Ｋ0，Ｋd）

暗号化暗号鍵Ｃkdk0として供給される場合がある。暗号鍵Ｋdが暗号化されて供給される場合には、暗号化暗号鍵Ｃkdk0を復号化するための共通暗号鍵Ｋ0がユーザに供給される。この共通暗号鍵Ｋ0の供給はユーザがデータベースに登録を行ったときに行われる場合と、暗号化データＣmkdが送られるときに暗号化データＣmkdとともにユーザに渡される場合がある。

【００２０】（ａ）暗号鍵が暗号化されていない場合。この暗号鍵システムにおいて、放送局１はデータベース２から供給された暗号鍵Ｋdを電波６を利用して放送する。受信装置４は受信した暗号鍵Ｋdをユーザ端末装置８に供給し、ユーザ端末装置８は受け取った暗号鍵Ｋdを半導体メモリ，フレキシブルディスクあるいはハード

ディスク等の記録媒体に保存する。データ利用希望者（ユーザ）はデータ通信装置５を用いて通信回線７を経由してデータベース２にデータＭの利用を申し込む。データＭの利用申し込みを受けたデータベース２は利用希望があったデータＭを許可鍵Ｋpである暗号鍵Ｋdを用いて暗号化し、

Ｃmkd＝Ｅ（Ｋd，Ｍ）

暗号化データＣmkdを通信回線７を経由してユーザのデータ通信装置５に送信するとともに課金センタ３との間で課金処理を行う。データ通信装置５は受け取った暗号化データＣmkdをユーザ端末装置８に供給し、ユーザ端末装置８は記録媒体に保存されていた暗号鍵Ｋdを用いて暗号化データＣmkdを復号化する。

Ｍ＝Ｄ（Ｋd，Ｃmkd）

【００２１】（ｂ）暗号鍵が暗号化され、共通暗号鍵が予めユーザに配布されている場合。

この暗号鍵システムにおいて、ユーザがデータベースを利用することを登録するときに、共通暗号鍵Ｋ0がＲＯＭあるいはフレキシブルディスク等の記録媒体によってユーザに供給され、供給された共通暗号鍵Ｋ0はユーザ端末装置８に保存されている。データベース２は暗号鍵Ｋdを共通暗号鍵Ｋ0を用いて暗号化し、

Ｃkdk0＝Ｅ（Ｋ0，Ｋd）

暗号化暗号鍵Ｃkdk0を放送局１に供給する。放送局１はデータベース２から供給された暗号化暗号鍵Ｃkdk0を電波６を利用して放送する。受信装置４は受信した暗号化暗号鍵Ｃkdk0をユーザ端末装置８に供給し、ユーザ端末装置８は初めに暗号化暗号鍵Ｃkdk0を予め保存されている共通暗号鍵Ｋ0を用いて復号化し、

Ｋd＝Ｄ（Ｋ0，Ｃkdk0）

復号された暗号鍵Ｋdを半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存する。

【００２２】データ利用希望者はデータ通信装置５を用いて通信回線７を経由してデータベース２にデータＭの利用を申し込む。データの利用申し込みを受けたデータベース２は利用希望があったデータＭを暗号鍵Ｋdを用いて暗号化し、

Ｃmkd＝Ｅ（Ｋd，Ｍ）

通信回線７を経由してデータ通信装置５に送信するとともに課金センタ３との間で課金処理を行う。データ通信装置５は受信した暗号化データＣmkdをユーザ端末装置８に供給し、ユーザ端末装置８は保存されていた暗号鍵Ｋdを用いて暗号化データＣmkdを復号化する。

Ｍ＝Ｄ（Ｋd，Ｃmkd）

【００２３】（ｃ）暗号鍵が暗号化されており、共通暗号鍵が暗号化データとともにユーザに配布される場合。

この暗号鍵システムにおいて、データベース２は共通暗号鍵Ｋ0を用いて暗号鍵Ｋdを暗号化し、

Ｃkdk0＝Ｅ（Ｋ0，Ｋd）

放送局１に供給する。放送局１はデータベース２から供給された暗号化暗号鍵ＣkdＫ0を電波６を利用して放送する。受信装置４は受信した暗号化暗号鍵Ｃkdk0をユーザ端末装置８に供給し、ユーザ端末装置８は暗号化暗号鍵ＣＫdk0を半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存しておく。

【００２４】データ利用希望者はデータ通信装置５を用いて通信回線７を経由してデータベース２にデータＭの利用を申し込む。データの利用申し込みを受けたデータベース２は利用希望があったデータＭを暗号鍵Ｋdを用いて暗号化し、

Ｃmkd＝Ｅ（Ｋd，Ｍ）

共通暗号鍵Ｋ0と一緒に通信回線７を経由してデータ通信装置５に送信するとともに課金センタ３との間で課金処理を行う。データ通信装置５は受信した暗号化データＣmkdと共通暗号鍵Ｋ0をユーザ端末装置８に供給し、ユーザ端末装置８は共通暗号鍵Ｋ0を用いて記録媒体に保存されていた暗号化暗号鍵Ｃkdk0を復号化し、

Ｋd＝Ｄ（Ｋ0，Ｃkdk0）

復号化された暗号鍵Ｋdを用いて暗号化データＣmkdを復号化する。

Ｍ＝Ｄ（Ｋd，Ｃmkd）

【００２５】

【発明の概要】本願においては、この先願に記載された暗号鍵システムの発明をテレビジョンシステム、データベースシステムあるいは電子商取引システム等に適用するための具体的な構成を提供する。このシステムは放送局、データベース、受信装置、データ通信装置及びユーザ端末装置から構成され、暗号鍵方式としては秘密鍵方式、公開鍵方式が採用され、さらにデジタル署名が用いられ、このとき用いられる暗号鍵は暗号化されあるいは暗号化されないで放送によって供給される。本発明は、データベースシステム、ペイパービューシステム、ビデオオンデマンドシステムにおける不正利用の防止、著作権の管理において有効であり、さらには電子情報情報システムを利用した電子マーケットの実現において有効な手段である。

【００２６】

【実施例】以下、図２～図４を用いて本願発明の実施例を説明する。

［第１実施例］図２に示されたのは本願発明をデータベースシステムに適用した第１実施例の暗号鍵システムであり、このシステムは、ＢＳ・ＣＳ・地上波テレビジョンあるいはＦＭ放送等による多重化放送あるいはデジタル放送によりデータ放送を行う放送局１１、動画データを含む種々のデータが蓄積されたデータベース１２、課金センタ１３、放送局１１が放送するデータ放送を受信する受信装置１４、データベース１２と通信を行うデータ通信装置１５及びデータを利用するユーザ端末装置１８から構成されている。

【００２７】データベース１２と放送局１１との間及びデータベース１２と課金センタ１３の間は専用回線等の通信回線で接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。データベース１２とデータ通信装置１５の間は公衆回線あるいはＣＡＴＶ回線等の通信回線１７で接続されている。放送局１１と受信装置１４の間は地上波テレビジョン放送、衛星テレビジョン放送、ＣＡＴＶ放送、ＦＭ放送あるいは衛星データ放送等の電波１６で接続されている。受信装置１４とユーザ端末装置１８との間及びデータ通信装置１５とユーザ端末装置１８との間は接続ケーブル等の直接的手段あるいはフレキシブルディスク等の間接的な手段により接続されている。この図において実線で示されたのは暗号化されていないデータの経路であり、破線で示されたのは暗号化されたデータの経路である。なお、データベース１２と放送局１１との間及びデータベース１２と課金センタ１３の間のデータの受け渡しは原則として専用回線あるいはフレキシブルディスクにより行われるが、この他に公衆回線あるいは放送衛星、通信衛星、地上波放送によって行うこともできる。その場合にデータは暗号化される。

【００２８】このシステムにおいては、暗号鍵方式として秘密鍵方式と公開鍵方式が採用される。データベース１２は公開鍵Ｋbdと専用鍵Ｋvdを用意し、放送局１１に公開鍵Ｋbdを供給する。公開鍵Ｋbdを受け取った放送局１１はアナログテレビジョン映像信号の帰線消去期間中の走査線を利用した文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用したデータ放送、ＦＭ多重データ放送あるいはデジタルデータ放送で公開鍵Ｋbdを放送する。なお、この場合公開鍵Ｋbdにデータベース１１のデジタル署名を行うようにすることもできる。

【００２９】このときにデータ利用の便のため、利用することができるデータのタイトルを記載した目次、データの内容紹介、商品カタログ、発注書、無記載の小切手、著作権情報を暗号化することなく供給することもできる。放送された公開鍵Ｋbdを受信した受信装置１４は、公開鍵Ｋbdをユーザ端末装置１８に転送し、転送された公開鍵Ｋbdを受け取ったユーザ端末装置１８は半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に公開鍵Ｋbdを保存する。

【００３０】目次あるいは内容紹介等によって利用を希望するデータを選択したユーザは、データ通信装置１５を用いて通信回線１７を経由してデータベース１２にデータＭの利用を申し込む。このときユーザは自分の秘密鍵Ｋsuを受信したデータベース１２の公開鍵Ｋbdを用いて暗号化し、

Ｃksukbd＝Ｅ（Ｋbd，Ｍksu）

データベース１２に送信する。

【００３１】データベース１２は、暗号化されたユーザの秘密鍵Ｃksukbdを専用鍵Ｋvdを用いて復号化し、

Ｋsu＝Ｄ（Ｋvd，Ｃksukbd）

利用申し込みがなされたデータＭを復号化されたユーザの秘密鍵Ｋsuを用いて暗号化し、

Ｃmksu＝Ｅ（Ｋsu，Ｍ）

通信回線１７を経由してユーザのデータ通信装置１５に送信する。

【００３２】自分の秘密鍵Ｋsuを用いて暗号化されたデータＣmksuを受け取ったユーザはユーザ端末装置１８で、自分の秘密鍵Ｋsuを用いて暗号化された暗号化データＣmksuを復号化し、

Ｍ＝Ｄ（Ｋsu，Ｃmksu）

利用する。

【００３３】このシステムにはデータベース１２に連動する課金センタ１３が設けられている。この課金センタ１３は、データが有料で提供される場合には利用されるが、データがショッピング情報等無料で提供されるデータである場合には利用されない。しかし、ショッピング情報等無料で提供されるデータであっても、受・発注にともなう代金清算が行われる場合には利用される。

【００３４】［第２実施例］図３に示されたのは、本願発明を利用希望者からの希望に応じてテレビジョン番組を放送するビデオオンデマンド（Video On Demand：ＶＯＤ）システムに適用した第２実施例の暗号鍵システムである。このシステムはＣＡＴＶ放送局２１、課金センタ２３、受信装置２４、データ通信装置２５及びユーザ端末装置２８から構成される。課金センタ２３は、テレビジョン番組が有料で提供される場合には利用されるが、テレビジョン番組が広告付き等無料で提供される場合には利用されない。このシステムにおいて、暗号化されたテレビジョン放送番組と暗号鍵とは単一の経路であるＣＡＴＶ回線２７で送信される。

【００３５】ＣＡＴＶ放送局２１と課金センタ２３の間は専用回線等の通信回線により電気的に接続する直接的手段あるいはフレキシブルディスク等の間接的な手段により接続されている。ＣＡＴＶ放送局２１と受信装置２４の間及びＣＡＴＶ放送局２１とデータ通信装置２５の間はＣＡＴＶ回線２７で接続されている。受信装置２４とユーザ端末装置２８との間及びデータ通信装置２５とユーザ端末装置２８との間は接続ケーブル等の直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。この図において実線で示されたのは暗号化されていないデータの経路であり、破線で示されたのは暗号化されたデータの経路である。なお、ＣＡＴＶ放送局２１と課金センタ２３の間のデータの受け渡しは原則として専用回線あるいはフレキシブルディスクにより行われるが、この他に公衆回線あるいは放送衛星、通信衛星、地上波放送によって行うこともできる。その場合にデータは暗号化される。

【００３６】このシステムにおいては、ＣＡＴＶシステムもデータベースの一種として扱われ、暗号鍵方式とし

て秘密鍵方式と公開鍵方式が採用される。このＶＯＤシステムを利用するユーザは自分の公開鍵ＫbuをＣＡＴＶ放送局２１に予め登録しておくかあるいは利用申込時に通信装置２５を用いて送信する。

【００３７】ＣＡＴＶ放送局２１は送信されたユーザの公開鍵Ｋbuを用いてＣＡＴＶ放送局２１の秘密鍵Ｋsbを暗号化し、

Ｃksbkbu＝Ｅ（Ｋbu，Ｋsb）

ＣＡＴＶ回線２７を経由してデータ通信装置２５に送信する。一方、テレビジョン番組ＭはＣＡＴＶ放送局２１の秘密鍵Ｋsbを用いて暗号化され、

Ｃmksb＝Ｅ（Ｋsb，Ｍ）

ＣＡＴＶ回線２７を経由して受信装置２４に放送される。

【００３８】ユーザは受信したＣＡＴＶ放送局２１の暗号化秘密鍵Ｃksbkbuをユーザの専用鍵Ｋvuを用いて復号化し、

Ｋsb＝Ｄ（Ｋvu，Ｃksbkbu）

復号されたＣＡＴＶ放送局２１の秘密鍵Ｋsbを用いて暗号化テレビジョン番組Ｃmksbを復号化し、

Ｍ＝Ｄ（Ｋsb，Ｃmksb）

利用する。

【００３９】また、この暗号鍵システムは暗号化が可能ならばＣＡＴＶ以外のテレビジョン放送、音声放送あるいはデータ放送に対しても適用可能である。また、放送局から暗号鍵を送信する方法として、アナログテレビジョン映像信号の帰線消去期間中の走査線を利用した文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用したデータ放送、ＦＭ多重データ放送あるいはデジタルデータ放送が利用可能である。

【００４０】さらに、この暗号鍵システムは本発明者らが提案した先願である特願平６－６４８８９号、特願平６－２３７６７３号、特願平６－２６４１９９号、特願平６－２６４２０１号、特願平６－２６９９５９号に記載されたデータ著作権管理システムにおいて暗号鍵を配布する場合にも利用可能である。また、この暗号鍵システムは特開平６－１３２９１６号公報に記載されている本発明者らが提案した、複数の情報が複数の異なるパターンで暗号化されて記録されているＣＤ－ＲＯＭ等の記録媒体を利用する場合にも適用可能である。これらの先願発明について説明する。

【００４１】特願平６－６４８８９号に記載されているデータ著作権管理システムの概要は次のようなものである。デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示（音声化を含む），保存，複写，加工，転送における著作権の管理を行うために、利用申し込み者に対して暗号化されたデータの利用を許可する鍵の他に、必要に応じて著作権を管理するためのプログラム，著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を送信する。著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【００４２】著作権管理プログラム，著作権情報及び著作権管理メッセージは、各々許可鍵とともに全体が供給される場合、データとともに全体が供給される場合及び一部が許可鍵とともに供給され、一部がデータとともに供給される場合がある。データ，許可鍵，著作権管理メッセージ、著作権情報及び著作権管理プログラムには、暗号化された状態で送信されるが利用時には暗号が解かれる場合、暗号化された状態で送信され表示の際のみに暗号が解かれその他の場合は暗号化された状態である場合、全く暗号化されない場合、の３つの場合がある。

【００４３】特願平６－２３７６７３号に記載されているデータ著作権管理システムの概要は次のようなものである。このデータベース著作権管理システムは、暗号化されていないデータが蓄積されたデータベース、データベースからの暗号化されたデータを放送する衛星放送局等の放送局あるいはデータベースの暗号化されたデータが記録されたＣＤ－ＲＯＭ等の記録媒体であるデータ供給手段、通信ネットワーク、暗号鍵を管理する鍵管理センタ、データベースの著作権を管理する著作権管理センタから構成され、データベースを利用するためのデータベース利用プログラムおよび著作権を管理するための著作権管理プログラム、第１の暗号鍵、第２の暗号鍵が使用される。

【００４４】１次ユーザはデータベースを利用するために予め鍵管理センタに登録を行い、その際にデータベース利用プログラムを配布されている。このデータベース利用プログラムには、１次ユーザに関する情報および情報を利用して所定のアルゴリズムにより１次ユーザ固有の暗号鍵を生成するプログラムが含まれている。データは暗号化されずにデータベースに蓄積されており、放送され、記録媒体に記録されあるいは通信ネットワークを経由することよって配布されるときに第１の暗号鍵で暗号化され、暗号化データとされる。暗号化データは、放送あるいは通信ネットワークを経由して配布された場合には１次ユーザ端末装置の半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存され、ＣＤ－ＲＯＭ記録媒体に記録されて配布された場合にはそのままの状態あるいは１次ユーザ端末装置の半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存される。

【００４５】データベースから直接にデータを利用する１次ユーザは通信ネットワークを経由して、鍵管理センタに暗号化データを復号化して利用するための鍵を要求するが、このときに１次ユーザに関する情報を提示する。鍵管理センタは１次ユーザに関する情報を著作権管

理センタに転送し、著作権管理センタは１次ユーザに関する情報Ｉを利用して所定のアルゴリズムにより１次ユーザ固有の暗号鍵を生成し、生成された１次ユーザ暗号鍵を利用して著作権管理プログラム、第１の暗号鍵および第２の暗号鍵を暗号化して、鍵管理センタに転送する。この１次ユーザに関する情報を利用して生成された暗号鍵を用いて暗号化された著作権管理プログラムは１次ユーザに固有のものである。

【００４６】暗号化された著作権管理プログラムを受け取った鍵管理センタは各々暗号化された著作権管理プログラム、第１の暗号鍵、第２の暗号鍵を１次ユーザ端末装置に対して通信ネットワークを経由して１次ユーザ端末装置に送信し、１次ユーザは受信した暗号化著作権管理プログラム、暗号化第１暗号鍵、暗号化第２暗号鍵を半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存する。

【００４７】１次ユーザは、予め配布されているデータベース利用プログラムを用い所定のアルゴリズムにより１次ユーザに関する情報を利用して１次ユーザ固有の暗号鍵を生成し、生成された暗号鍵を用いて暗号化著作権管理プログラム、暗号化第１暗号鍵および暗号化第２暗号鍵を復号化し、復号された第１の暗号鍵を用いて暗号化データを復号化する。

【００４８】以後復号されたデータの保存、コピーあるいは転送を行う場合には復号された著作権管理プログラムにより復号された第２暗号鍵を用いて暗号化が行われ、暗号化データが１次ユーザ端末装置内の半導体メモリ、フレキシブルディスクあるいはハードディスク等の記録媒体に保存され、１次ユーザが保存された暗号化データを利用するときには第２暗号鍵を用いて復号化し、この操作が繰り返されて１次利用が行われる。

【００４９】暗号化データが外部記憶媒体にコピーされたときあるいは通信ネットワークを経由して２次ユーザ端末装置に転送された場合には、著作権管理プログラムにより第１暗号鍵および第２暗号鍵が廃棄され、１次ユーザは暗号化データを利用することができなくなる。このとき、暗号化データが１次ユーザ端末装置に保存されている場合には、保存されている暗号化データに、１次ユーザについての暗号化されていない情報が付加される。

【００５０】１次ユーザが再度暗号化データを利用する場合には、著作権管理センタから第１暗号鍵と第２暗号鍵の再交付を受け、この再交付が行われたことにより、この１次ユーザから暗号化データのコピーあるいは転送を受けた２次ユーザが存在することが確認され、２次ユーザの存在が著作権管理センタに記録される。

【００５１】コピーあるいは転送された暗号化データを受け取った２次ユーザは著作権管理センタに暗号化データの２次利用を申込む。２次ユーザは１次ユーザと異なり予め鍵管理センタに登録をしておく必要はなく、利用申込時に暗号化データのコピーあるいは転送を受けた１次ユーザの情報を著作権管理センタに提示することにより利用申込が受理される。このときに１次ユーザ情報が提示されない場合には、そのユーザは１次ユーザから暗号化データのコピーあるいは転送を受けた２次ユーザではなく、１次ユーザであると認められるため、その２次利用申込は受理されない。２次利用申込を受理した著作権管理センタは暗号化データを復号化するための第２暗号鍵、復号された暗号化データを再暗号化および再復号化するための第３暗号鍵、これらの復号化、再暗号化、再復号化を行う著作権管理プログラムを２次ユーザに送信する。

【００５２】特願平６－２６４１９９号に記載されている著作権管理システムの概要は次のようなものである。この著作権管理システムにおいては、ユーザが用意する第１の公開鍵，第１の公開鍵に対応する第１の専用鍵，第２の公開鍵，第２の公開鍵に対応する第２の専用鍵とデータベース側が用意する第１の秘密鍵及び第２の秘密鍵が使用される。

【００５３】データベース側では、暗号化されていないデータを第１の秘密鍵を用いて暗号化し、第１の秘密鍵を第１の公開鍵を用いて暗号化するとともに第２の秘密鍵を第２の公開鍵を用いて暗号化し、これらの暗号化されたデータ，暗号化第１秘密鍵及び暗号化第２秘密鍵をユーザに送信する。

【００５４】ユーザは、暗号化第１秘密鍵を第１専用鍵を用いて復号化し、復号化された第１秘密鍵を用いて暗号化データを復号化し、利用するとともに、暗号化された第２秘密鍵を第２専用鍵を用いて復号化し、復号化第２秘密鍵は復号化以降におけるデータの保存・複写・転送時の暗号鍵として使用される。

【００５５】特願平６－２６４２０１号に記載されているデータ著作権管理システムの概要は次のようなものである。データベースから入手した複数の暗号化されたデータを加工することにより新しいデータを作成し、暗号化して他人に供給する場合に、原材料である複数のデータの暗号鍵と、加工プロセスである加工プログラムをデジタル署名化したデータを利用許可鍵として使用する。加工され暗号化されたデータを受け取ったユーザが著作権管理センタにデジタル署名を提示して利用申込を行うと、著作権管理センタはデジタル署名に基づいて加工者を確認し、加工者が被加工データの正当なユーザであることが確認された場合にのみ、利用申込者に対して利用のための暗号鍵を提供する。

【００５６】特願平６－２６９９５９号に記載されている方法の概要は次のようなものである。１次ユーザはデータベースから原データが第１の暗号鍵で暗号化された暗号化データを受け取り、復号化して利用するが、その後は第１の暗号鍵、１次ユーザデータ、データ利用回数の内の１つあるいはこれらを組み合わせて所定のアルゴ

リズムにより生成された第２の暗号鍵で暗号化されて保存、複写、転送が行われる。２次ユーザがデータの２次利用を要求すると著作権管理センタは原データの第１の暗号鍵、１次ユーザデータ、データ利用回数の内の１つあるいはこれらを組み合わせて所定のアルゴリズムにより第２の暗号鍵を生成し２次ユーザに提供する。第２の暗号鍵を提供された２次ユーザは、第２の暗号鍵を用いて暗号化された原データを復号化し、利用する。

【００５７】［第３実施例］図４に示されたのは本願発明をデータベースシステムあるいはＶＯＤシステムに適用した第３実施例の暗号鍵システムである。この暗号鍵システムも図３に示された第２実施例の暗号鍵システムと同様に暗号鍵とテレビジョン放送番組とはＣＡＴＶ回線である単一の経路を通るが、これらを異なる経路を通るようにすることが可能であることはもちろんのことである。このシステムはデータ放送を行うＣＡＴＶ放送局３１、データベースあるいはビデオシステム等のデータ管理センタ３３、受信装置３４、データ通信装置３５及びユーザ端末装置３８から構成される。

【００５８】データ管理センタ３３とＣＡＴＶ放送局３１の間は専用回線等の通信回線で接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。ＣＡＴＶ放送局３１と受信装置３４の間及びＣＡＴＶ放送局３１とデータ通信装置３５の間はＣＡＴＶ回線３７で接続されている。なお、ＣＡＴＶ回線３７に代えて他の適当なデータ放送あるいはデータ通信可能な通信回線を使用することが可能である。受信装置３４とユーザ端末装置３８との間及びデータ通信装置３５とユーザ端末装置３８との間は接続ケーブル等の直接的な手段あるいはフレキシブルディスク等の間接的な手段により接続されている。この図において実線で示されたのは暗号化されていないデータの経路であり、破線で示されたのは暗号化されたデータの経路である。なお、データ管理センタ３３とＣＡＴＶ放送局３１の間のデータの受け渡しは原則として専用回線あるいはフレキシブルディスクにより行われるが、この他に公衆回線あるいは放送衛星、通信衛星、地上波放送によって行うこともできる。その場合にデータは暗号化される。

【００５９】このシステムにおいて採られる暗号鍵方式は秘密鍵方式と公開鍵方式である。データ管理センタ３３は供給される全データに共通する公開鍵Ｋbd及び専用鍵Ｋvdとデータ各々で異なる秘密鍵Ｋsdiを用意しＣＡＴＶ放送局３１に供給する。ＣＡＴＶ放送局３１は受け取った秘密鍵Ｋsdiをデータ管理センタ３３の公開鍵Ｋbdを用いて暗号化して、

Ｃksdikbd＝Ｅ（Ｋbd，Ｋsdi）

アナログテレビジョン映像信号の帰線消去期間中の走査線を利用した文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用したデータ放送、ＦＭ多重データ放送あるいはデジタルデータ放送により放送する。このときにデータ利用の便のため、利用することができるデータのタイトルを記載した目次、あるいはデータの利用を促進するため、データの概要を説明する内容紹介を暗号化することなく供給することもできる。

【００６０】目次あるいは内容紹介によって利用を希望するデータを選択したユーザは、データ通信装置３５を用いてＣＡＴＶ回線３７を経由しＣＡＴＶ放送局３１を介してデータ管理センタ３３にデータの利用を申し込む。このときユーザは自分の公開鍵Ｋbuをデータ管理センタ３３に送信する。ユーザからの利用申し込みを受けたデータ管理センタ３３は秘密鍵Ｋsdiを用いてデータＭを暗号化して

Ｃmksdi＝Ｅ（Ｋsdi，Ｍ）

ユーザ端末装置３８に送信する。その時データ管理センタの専用鍵Ｋvdが利用申し込みを行ったユーザの公開鍵Ｋbuを用いて暗号化され、

Ｃkvdkbu＝Ｅ（Ｋbu，Ｋvd）

ユーザ端末装置３８に送信される。

【００６１】データ管理センタの暗号化専用鍵Ｃkvdkbuを受け取ったユーザは、データ管理センタの暗号化専用鍵Ｃkvdkbuをユーザの専用鍵Ｋvuを用いて復号化し、

Ｋvd＝Ｄ（Ｋvu，Ｃkvdkbu）

復号化されたデータ管理センタの専用鍵Ｋvdを用いて暗号化秘密鍵Ｃksdikbdを復号化し、

Ｋsdi＝Ｄ（Ｋvd，Ｃksdikbd）

復号されたデータ管理センタの秘密鍵Ｋsdiを用いて暗号化データＣmksdiを復号化して

Ｍ＝Ｄ（Ｋsdi，Ｃmksdi）

利用する。

【００６２】［第４実施例］第４実施例のシステム構成は図４に示された第３実施例と同じであるから説明は省略する。このシステムにおいて採られる暗号鍵方式は第３実施例と同様に秘密鍵方式と公開鍵方式であるが、第３実施例では利用申し込みを行ったユーザの公開鍵Ｋbuでデータ管理センタの専用鍵Ｋvdが暗号化されてユーザに送信されるのに対し、第４実施例においてはデータ管理センタの専用鍵Ｋvdが予めＩＣカード等を用いて配布されユーザ端末装置内に保存されている点及び第３実施例においてはデータＭがデータの利用を申し込みに対応して配信されるのに対し、第４実施例ではデータＭがＣＡＴＶ回線あるいは衛星放送により利用希望とは無関係に放送される点で異なる。

【００６３】ユーザがデータ管理センタとデータベースを使用する包括的な契約を締結する際に、供給される全データに共通するデータ管理センタの専用鍵ＫvdがＩＣカード等の記録媒体によりあるいはＣＡＴＶ回線３７を経由して予めユーザに配布され、ユーザ端末装置３８内の半導体メモリ，ハードディスク装置あるいはフレキシブルディスクに保存されている。データ管理センタ３３は公開鍵Ｋbdと供給されるデータ各々で異なる秘密鍵Ｋ

sdiを用意しＣＡＴＶ放送局３１に供給する。秘密鍵Ksdiを受け取ったＣＡＴＶ放送局３１はその秘密鍵Ksdiを公開鍵Kbdを用いて暗号化し、

Cksdikbd＝Ｅ（Kbd，Ksdi）

暗号化秘密鍵Ksdikbdをアナログテレビジョン映像信号の帰線消去期間中の走査線を利用した文字多重放送、アナログテレビジョン音声信号の副音声帯域を利用したデータ放送、ＦＭ多重データ放送あるいはデジタルデータ放送により放送する。このときにデータ利用の便のため、利用することができるデータのタイトルを記載した目次、あるいはデータの利用を促進するため、データの概要を説明する内容紹介を暗号化することなく供給することもできる。

【００６４】ＣＡＴＶ放送局３１は、秘密鍵Ksdiを用いてデータＭを暗号化し、

Cmksdi＝Ｅ（Ksdi，Ｍ）

ＣＡＴＶ回線により利用希望とは無関係に一方的に放送する。ユーザは、目次あるいは内容紹介に基づきＣＡＴＶ回線で放送されているデータの中から希望するデータを受信装置３４を用いてユーザ端末装置３８に取り込む。

【００６５】ユーザは予め配布されてユーザ端末装置３８内の半導体メモリ，ハードディスク装置あるいはフレキシブルディスクに保存されているデータ管理センタの専用鍵Kvdを用いて暗号化秘密鍵Cksdikbdを復号化し、

Ksdi＝Ｄ（Kvd，Cksdikbd）

復号化された秘密鍵Ksdiを用いて暗号化データCmksdiを復号化し、

Ｍ＝Ｄ（Ksdi，Cmksdi）

利用する。

【００６６】暗号鍵を配布するためのその他の変形実施例を説明する。

［第５実施例］これまでに説明した実施例において、データ管理センタの公開鍵Kbdは通信回線経由ではなく放送局から放送されるため、それが真正なものであるか否か確認することができない。そのような場合にはデータ管理センタの公開鍵Kbdにデータ管理センタの専用鍵Kvdを用いてデジタル署名を行い、

Skbdkvd＝Ｅ（Kvd，Kbd）

データ管理センタの公開鍵Kbdとともにデジタル署名Skbdkvdを放送する。ユーザは、受信したデータ管理センタの公開鍵Kbdを用いてデジタル署名Skbdkvdを確認し、

Kbd＝Ｄ（Kbd，Skbdkvd）

それが真正なものであれば使用する。

【００６７】［第６実施例］第５実施例においてデータ管理センタがデータベースの利用を予め登録する会員制を採用している場合には、さらに会員であるユーザの公開鍵Kbuiを予めデータ管理センタに登録しておく。データ管理センタは、データ管理センタの公開鍵Kbdを各ユーザの公開鍵Kbuiを用いて暗号化する。

Ckbdkbui＝Ｅ（Kbui，Kbd）

また、データ管理センタの公開鍵Kbdにデータ管理センタの専用鍵Kvdを用いてデジタル署名を行い、

Skbdkvd＝Ｅ（Kvd，Kbd）

ユーザ毎に異なる暗号化公開鍵Ckbdkbui及びデジタル署名Skbdkvdを放送局に送り、放送局は受け取った暗号化公開鍵Ckbdkbui及びデジタル署名Skbdkvdを放送する。このとき、必要ならば各ユーザの暗号化されていないユーザ識別情報を暗号化公開鍵Ckbdkbuiに付与して放送する。放送された暗号化公開鍵Ckbdkbui及びデジタル署名Skbdkvdを受け取ったユーザはそのユーザの公開鍵Kvuiを用いてデータ管理センタの暗号化公開鍵Ckbdkbuiを復号化し、

Kbd＝Ｄ（Kvui，Ckbdkbui）

復号化されたデータ管理センタの公開鍵Kbdをユーザの端末装置内に保存しておく。また、ユーザは、受信したデータ管理センタの公開鍵Kbdを用いてデジタル署名Skbdkvdを確認し、

Kbd＝Ｄ（Kbd，Skbdkvd）

それが真正なものであれば保存されていたデータ管理センタの公開鍵Kbdを使用する。このようにすると、ユーザ個々に異なる暗号鍵を配布することができる。

【００６８】［第７実施例］ユーザはデータ管理センタにアクセスする毎に又はリクエストする毎に自分の公開鍵Kbuをデータ管理センタに提示する。ユーザからのリクエストを受けたデータ管理センタは要求されたデータＭをユーザの公開鍵Kbuを用いて暗号化し、

Cmkbu＝Ｅ（Kbu，Ｍ）

放送局に送り、放送局は受け取った暗号化データCmkbuを放送する。放送された暗号化データCmkbuを受信したユーザはユーザの専用鍵Kvuを用いて復号化して、

Ｍ＝Ｄ（Kvu，Cmkbu）

利用する。

【００６９】図５を用いて、本願発明の暗号鍵システムを使用した応用例を示す。この図に示された各応用例は電子情報交換システムを利用する電子マーケット取引に、（ａ）に示されたものは小売店が行うクレジット決済に、（ｂ）に示されたのは電子小切手による決済に、（ｃ）に示されたのはメーカ等が行う卸売販売に、各々これらの暗号鍵システムを適用した場合の構成である。これらのシステムは、秘密鍵方式に加えてデジタル署名が利用され、ユーザ４２、インターネット上のWWW（World Wide Web）サーバである小売店４３、金融機関４４あるいはメーカ等である卸売店４５から構成される。

【００７０】［第８実施例］（ａ）に示された小売店におけるクレジット決済において、小売店４３は発注書のフォーマット、クレジットカードフォーマット、広告、

カタログ、予告編、製品説明、データベースの内容紹介や目次／料金表／価格表などのデータMsを衛星４１あるいはＣＡＴＶ回線を経由して放送する。発注書フォーマット等のデータMs及び小売店４３の公開鍵Kbsを受け取ったユーザ４２は、小売店４３の公開鍵Kbsを用いてユーザの秘密鍵Ksuを暗号化し、

Cksukbs＝Ｅ（Kbs，Ksu）

広告、カタログ、製品説明、料金価格表等の情報に基づいて注文内容、支払金額、クレジットカード番号等の事項Muを発注書にユーザ４２の秘密鍵Ksuを用いて暗号化して記入し、

Cmuksu＝Ｅ（Ksu，Mu）

必要に応じて事項Muを圧縮文書muにしてユーザ４２の専用鍵Kvuを用いてデジタル署名を行い、

Smukvu＝Ｅ（Kvu，mu）

ユーザ４２の公開鍵Kbuを添付してネットワーク４７を経由して小売店４３に送信する。

【００７１】発注書等を受け取った小売店４３は、小売店４３の専用鍵Kvsを用いてユーザ４２の暗号化秘密鍵Cksukbsを復号化し、

Ksu＝Ｄ（Kvs，Cksukbs）

復号化されたユーザ４２の秘密鍵Ksuを用いて暗号化発注書Cmuksuを復号化し、

Mu＝Ｄ（Ksu，Cmuksu）

受注処理を実行する。さらにユーザ４２が添付した公開鍵Kbuを用いてユーザ４２のデジタル署名Smukvuを確認し、

mu＝Ｄ（Kbu，Smukvu）

ユーザ４２にネットワーク４７を経由してレシートを返信する。このシステムでは、発注書に記入されるクレジットカード番号を暗号化して送付しているためクレジット番号の盗用を防止することができる。

【００７２】また、小売店４３が発注書フォーマット、クレジットカードフォーマット、広告、カタログ、予告編、製品説明、データベースの内容紹介や目次／料金表／価格表などのデジタルデータMs1を圧縮文書ms1とし、これに小売店４３の専用鍵Kvsを用いてデジタル署名を行い、

Sms1kvs＝Ｅ（Kvs，ms1）

小売店４３の公開鍵Kbsを添付して放送し、ユーザが小売店４３の公開鍵Kbsを用いてデジタル署名Sms1kvsを確認

ms’＝Ｄ（Kbs，Smskvs）

するようにすることにより、取引がより確実なものとなる。

【００７３】［第９実施例］（ｂ）に示された電子小切手による決済において、金融機関４４はデジタルデータである無記載小切手フォーマットMfに金融機関４４の公開鍵Kbfを添付して衛星４１あるいはＣＡＴＶ回線を経由して放送する。無記載小切手フォーマットMfを受信したユーザ４２は、金融機関の公開鍵Kbfを用いてユーザ４２の秘密鍵Ksuを暗号化し、

Cksukbf＝Ｅ（Kbf，Ksu）

支払先と支払金額についての事項Muをユーザ４２の秘密鍵Ksuを用いて暗号化して記入し、

Cmuksu＝Ｅ（Ksu，Mu）

必要に応じて事項Muを圧縮文書muとし、これにユーザ４２の専用鍵Kvuを用いてデジタル署名を行って

Smukvu＝Ｅ（Kvu，mu）

ユーザ４２の公開鍵Kbuと、金融機関４４の公開鍵Kbfで暗号化されたユーザ４２の暗号化秘密鍵Cksukbfを添付してネットワーク４７を経由して金融機関４４に送信する。

【００７４】記載済み小切手を受け取った金融機関４４は、金融機関の専用鍵Kvfを用いてユーザ４２の暗号化秘密鍵Cksukbfを復号化し、

Ksu＝Ｄ（Kvf，Cksukbf）

復号化されたユーザの秘密鍵Ksuを用いて支払先と支払金額の暗号化データCmuksuを復号化し、

Mu＝Ｄ（Ksu，Cmuksu）

記載された内容を確認し、為替交換処理を実行する。さらにデジタル署名Smukvuが有るものはユーザ４２が添付した公開鍵Kbuを用いてユーザ４２を確認し、

mu’＝Ｄ（Kbu，Smuksu）

確認書Ms2をユーザ４２が添付した公開鍵Kbuを用いて暗号化し、

Cms2kbu＝Ｅ（Kbu，Ms2）

ネットワーク４７を経由してユーザ４２に返信する。

【００７５】金融機関４４からの暗号化確認書Cms2kbuを受け取ったユーザは、ユーザ４２の専用鍵Kvuを用いて暗号化確認書Cms2kbuを復号化して

Ms2＝Ｄ（Kvu，Cms2kbu）

内容を確認する。このシステムによれば、支払先と支払金額を暗号化して小切手に記入しているため小切手に記載された内容の盗用を防止することができる。

【００７６】また、デジタルデータである無記載小切手フォーマットMfを圧縮文書mfとし、これに金融機関４４の専用鍵Kvfを用いてデジタル署名を行い、

Smfkvf＝Ｅ（Kvf，mf）

金融機関４４の公開鍵Kbfを添付して放送し、ユーザが金融機関４４の公開鍵Kbfを用いてデジタル署名Smskvfを確認

mf’＝Ｄ（Kbf，Smfkvf）

するようにし、さらに確認書Msを圧縮文書msとし、これにユーザが添付した公開鍵Kbuを用いてデジタル署名を行う

Smskbu＝Ｅ（Kbu，ms）

ようにすることにより、金融機関が記入者を確認することができる。

【００７７】［第１０実施例］（ｃ）に示されたメーカ

等の卸売店４５において、卸売店４５は見積依頼書フォーマットMw1を圧縮データmw1としこれに卸売店４５の専用鍵Kvwを用いてデジタル署名を行い、
Smw1kvw＝E（Kvw，mw1）
卸売店４５の公開鍵Kbwを添付して衛星４１あるいはＣＡＴＶ回線を経由して放送する。放送された見積依頼書フォーマットMw1と卸売店４５の公開鍵Kbwを受け取った小売店であるユーザ４２は、見積依頼書Muを卸売店４５の公開鍵Kbwを用いて暗号化し、
Cmukbw＝E（Kbw，Mu）
ネットワーク４７を経由して卸売店４５に送信する。このとき、必要に応じて見積依頼書Muを圧縮データmuとし、これにユーザ４２の専用鍵Kvuを用いてデジタル署名を行って、
Smkvu＝E（Kvu，mu）
ユーザ４２の公開鍵Kbuとともに卸売店４５に送信する。

【００７８】暗号化見積依頼書Cmukbwを受け取った卸売店４５は、卸売店４５の専用鍵Kvwを用いて暗号化見積依頼書Cmukbwを復号化し、
Mu＝D（Kvu，Cmukbw）
記載された見積依頼内容Muを確認し、見積作業を実行する。さらにデジタル署名Smkvuがされている場合には送信されたユーザ４２の公開鍵Kbuを用いてデジタル署名を確認し、
mu＝D（Kbu，Smkvu）
見積依頼書を確認する。見積作業を行った卸売店４５は、見積書Mw2をユーザ４２の公開鍵Kbuを用いて暗号化し、
Cmw2kbu＝D（Kbu，Mw2）
ネットワーク４７を経由してユーザ４２に送信する。

【００７９】卸売店４５の暗号化見積書Cmw2kbuを受け取ったユーザ４２は、ユーザ４２の専用鍵Kvuを用いて復号化する。
Mw2＝D（Kvu，Cmw2kbu）
このシステムによれば、公開鍵と専用鍵を使用しているため、見積書の内容が盗用されるおそれがなく、ユーザ毎に異なる見積を行うことができる。

【００８０】これら（ａ）～（ｃ）に示されたシステムにおいては、秘密性を要しない各種フォーマット及び広告とを衛星放送あるいはＣＡＴＶ放送によって放送するため、データの送信を効果的に行うことができる。

【００８１】以上説明したように、本発明の暗号鍵システムを用いることによりこれまで別々にシステムとして存在してきたテレビジョン放送あるいは音声放送等の一般的な情報メディアとコンピュータを用いたデータ通信メディアとを融合したマルティメディアシステムを実現することができる。以下、マルティメディアシステムを実現した具体的な構成を説明する。

【００８２】現行のテレビジョン放送は地上波放送、衛星放送あるいはＣＡＴＶ放送によりアナログ方式で行われ、一方最も一般的なデータ通信回線は電線を利用した公衆回線である。このようなシステム構成においてビデオオンデマンドを実現するシステムとして基本的な構成は図２に示された第１実施例の暗号鍵システムを利用することができる。放送局はアナログテレビジョン放送番組の垂直帰線期間の走査線にあるいは音声帯域の副音声帯域に多重して放送局の公開鍵Kbbを放送する。

【００８３】テレビジョン番組利用希望者は自分の秘密鍵Ksuを放送された放送局の公開鍵Kbbを用いて暗号化し、
Cksukbb＝E（Kbb，Ksu）
暗号化秘密鍵Cksukbbを通信回線を経由して放送局に送信して利用申込を行う。

【００８４】放送局は放送局の専用鍵Kvbを用いて利用希望者の暗号化秘密鍵Cksukbbを復号化し、
Ksu＝D（Kvb，Cksukbb）
復号された秘密鍵Ksuを用いて放送番組をスクランブルし、放送する。

【００８５】利用希望者は自分の秘密鍵Ksuを用いてスクランブルされた放送番組のスクランブルを解除して利用する。このような構成を採ることにより、利用希望者以外の者が番組を利用することは不可能になる。

【００８６】このようなシステム構成においてビデオオンデマンド及びペイパービューを実現するシステムとして基本的な構成は図４に示された第４実施例あるいは第５実施例の暗号鍵システムを利用することができる。放送局３１はアナログテレビジョン放送番組の垂直帰線期間の走査線に、あるいは音声帯域の副音声帯域に多重して放送局３１の公開鍵Kbbを用いて放送局３１の秘密鍵Ksbを暗号化し、
Cksbkbb＝E（Kbb，Ksb）
通信回線３７を経由して放送する。

【００８７】テレビジョン番組利用希望者３８は自分の公開鍵Kbuを通信回線３７を経由して放送局３１に送信して利用申込を行う。放送局３１は放送局の秘密鍵Ksbを用いて放送番組をスクランブルし、通信回線３７を経由して放送する。そのとき放送局３１の専用鍵Kvbが利用希望者３８の公開鍵Kbuで暗号化され
Ckvbkbu＝E（Kbu，Kvb）
通信回線３７を経由して放送される。

【００８８】利用希望者３８は自分の専用鍵Kvuを用いて放送局３１の暗号化専用鍵Ckvbkbuを復号化し、
Kvb＝D（Kvu，Ckvbkbu）
復号された放送局３１の専用鍵Kvbを用いて放送局３１の暗号化秘密鍵Cksbkbbを復号化し、
Ksb＝D（Kvb，Cksbkbb）
復号された放送局３１の秘密鍵Ksbを用いてスクランブルされた放送番組のスクランブルを解除して利用する。このような構成を採ることにより、利用希望者以外の者

が番組を利用することは不可能になる。

【００８９】さらに、この暗号鍵システムは最近盛んに行われているテレビジョン放送と電話とを組み合わせたテレビショッピングにも適用することができる。現在行われているアナログテレビジョン放送を利用したテレビジョンショッピングは、テレビジョン画面に商品紹介と販売方法を表示し、利用者は販売方法に関する情報を手で記録し、記録された情報に基づいて電話を用いて購入申込を行っている。これに対して、本発明の暗号鍵システムにおいてはアナログテレビジョン放送の垂直帰線期間の走査線あるいは音声帯域の副音声帯域に発注書フォーマット、小切手フォーマットのデータを多重して送信することを提案する。一方、パーソナルコンピュータとテレビジョン装置を一体化したパソコンテレビと呼ばれる装置、あるいはＩＣカード、ＰＣカードあるいは挿入ボードとして実現されるビデオキャプチャ装置とパーソナルコンピュータを組み合わせた装置により、テレビジョン画像を取り込むことが行われている。

【００９０】これらの発注書フォーマット、小切手フォーマットの多重データとビデオキャプチャ装置を組み合わせることにより電子的にテレビショッピングを行うことができる。このテレビショッピングにおいて、テレビショッピングの商品紹介画面が放送されているときに、垂直帰線期間の走査線あるいは音声帯域の副音声帯域で発注書フォーマット、小切手フォーマットがデータ多重されて放送される。購入を希望する商品の紹介画面が表示されているときに、利用者が操作をするとその静止画面とともに発注書フォーマット、小切手フォーマットのデータが取り込まれる。利用者は取り込まれた発注書フォーマット、小切手フォーマットに必要事項を記入し、購入申込を行う。このとき取引の安全性を図るために第１実施例から第５実施例に説明されたシステムにより、公開鍵方式あるいは秘密鍵方式による暗号化及びデジタル署名が行われる。このとき、発注書及び小切手とともに商品紹介の静止画面を添付して購入申込を行うようにすれば、取引内容の確認を行うことができる。

【００９１】簡易な方法としては、発注書フォーマット及び小切手フォーマットもテレビジョン画像として送信し、静止画面として取り込まれた発注書フォーマット及び小切手フォーマットに必要事項を記入するようにしてもよい。また、発注書フォーマット及び小切手フォーマットは音声帯域の副音声帯域に多重されるファクシミリ放送で送信することもできる。

【００９２】このような方法を採用することにより、テレビショッピングにより、現行のアナログテレビジョン方式によっても電子情報交換（ＥＤＩ）を利用した電子マーケットを実現することができる。

【００９３】これらのビデオオンデマンドシステム及びペイパービューシステムはアナログテレビジョン放送以外のデジタルテレビジョン放送に対しても適用可能である。通信回線としてＣＡＴＶ回線を使用した場合には放送とデータ通信の双方をこのＣＡＴＶ回線のみによって行うことが可能である。

【００９４】また、これらのビデオオンデマンドシステム及びペイパービューシステムは、低速の一般公衆回線あるいは高速のＩＳＤＮ（Integrated Services Digital Network）回線を利用したコンピュータ通信ネットワークシステム、さらには複数のコンピュータ通信ネットワークシステムを接続したインターネットシステムにおいて行われている高品質音声データ及び動画データの送受信に対しても適用可能である。

【００９５】使用する装置としてはテレビジョン受像装置に受信装置及び通信装置を組み込むこともできるが、セットトップボックス等を用いて別体に構成することもできる。また、最近徐々に普及しつつあるパーソナルコンピュータとテレビジョン装置を一体化したパソコンテレビと呼ばれる装置、あるいはパーソナルコンピュータにテレビジョン信号を送り込むＩＣカード、ＰＣカードあるいは挿入ボードとして実現されるビデオキャプチャ装置を組み合わせて構成することもできる。

【図面の簡単な説明】

【図１】先願発明の暗号鍵システムの構成図。

【図２】本願発明第１実施例の暗号鍵システムの構成図。

【図３】本願発明第２実施例の暗号鍵システムの構成図。

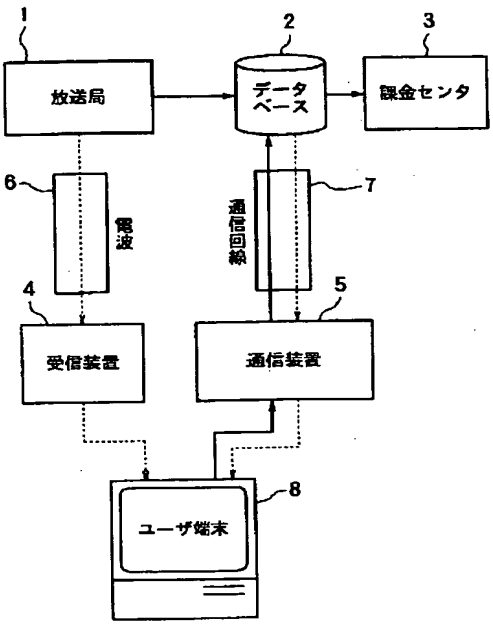
【図４】本願発明第３実施例及び第４実施例の暗号鍵システムの構成図。

【図５】本願発明を応用した第５実施例の構成図。

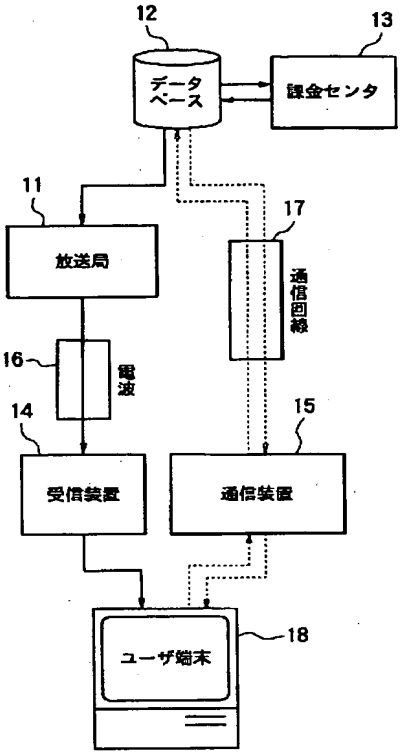
【符号の説明】

１，１１　放送局
２，１２　データベース
３，１３，２３　課金センタ
４，１４，２４，３４　受信装置
５，１５，２５，３５　データ通信装置
６，１６　電波
７，１７，２７，３７，４７　通信回線
８，１８，２８，３８　ユーザ端末装置
２１，３１　ＣＡＴＶ局
３３　管理センタ
４１　人工衛星
４２　ユーザ
４３　小売店
４４　金融機関
４５　卸売店

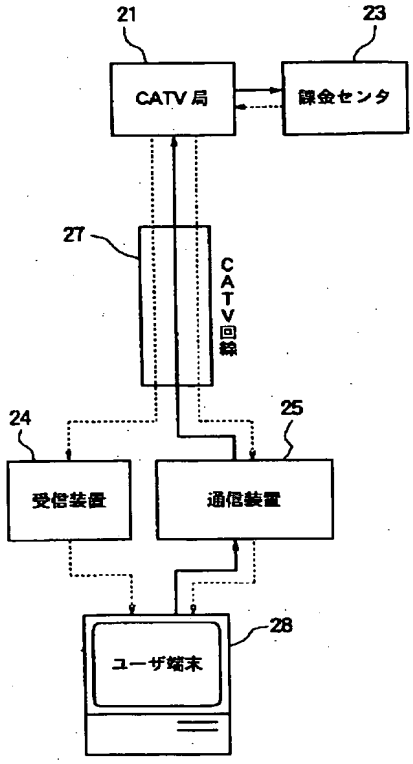
【図１】


1
2
3
放送局
データベース
課金センタ
6
電波
通信回線
7
4
5
受信装置
通信装置
8
ユーザ端末

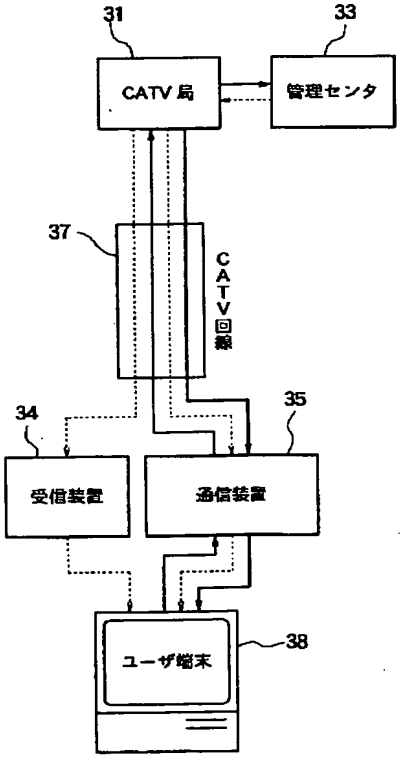
【図２】


12
13
データベース
課金センタ
11
17
放送局
通信回線
16
電波
14
15
受信装置
通信装置
18
ユーザ端末

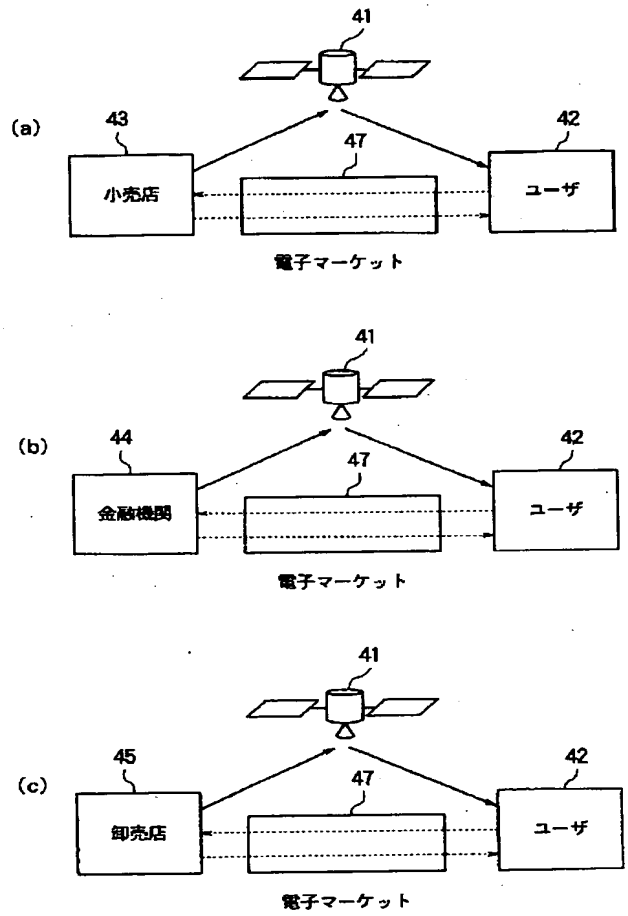
【図３】


21
23
CATV局
課金センタ
27
CATV回線
24
25
受信装置
通信装置
28
ユーザ端末

【図４】


31
33
CATV局
管理センタ
37
CATV回線
34
35
受信装置
通信装置
38
ユーザ端末

【図５】



フロントページの続き

(51) Int. Cl. 6	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｎ　7/167		8842－5Ｊ	Ｈ０４Ｌ　9/00	６０１Ｆ	
			Ｈ０４Ｎ　7/167	Ｚ	

Third Embodiment

[0057] Fig. 4 illustrates a third embodiment of cryptographic key system, in which the present invention is applied to a database system or VOD system. In the present cryptographic key system, similarly to the second embodiment of cryptographic key system as illustrated in Fig. 3, encrypted keys and television broadcast programs are transmitted through a single path, which is a CATV line, but, as a matter of course, they may be transmitted through different paths. The present system comprises a CATV broadcast station 31 for performing data broadcasts; a data management center 33 of a database, video system or the like; a receiver apparatus 34; a data communication apparatus 35; and a user terminal apparatus 38.

[0058] The connection between the data management center 33 and the CATV broadcast station 31 is achieved by using direct means that uses a communication line, such as a private line or the like, to connect them or by using indirect means, such as a flexible disc or the like. The connection between the CATV broadcast station 31 and each one of the receiver apparatus 34 and data communication apparatus 35 is achieved by using a CATV line 37. It should be noted that the CATV line 37 may be replaced by any other appropriate communication line that can support data broadcast or data communication. The connection between the user terminal apparatus 38 and each one of the receiver apparatus 34 and data communication apparatus 35 is achieved by using direct means that uses a connection cable or the like, or by using indirect means, such as a flexible disc or the like. In Fig. 4, solid lines designate paths of non-encrypted data, while dashed lines designate paths of encrypted data. It should be noted that although the data transmission and reception between the data management center 33 and the CATV broadcast station 31 are implemented by using, in general, a private line or flexible discs, yet they may be implemented alternatively by using a public line, a broadcast satellite, a communication satellite or a terrestrial broadcast. In such a case, the data

are encrypted.

[0059] The cryptographic key methods as employed in the present system are a secret key method and a public key method. The data management center 33 prepares public and private keys K_{bd} and K_{vd}, respectively, common to all the data to be supplied therefrom as well as different secret keys K_{sdi} used for respective data, and supplies them to the CATV broadcast station 31. The CATV broadcast station 31 uses the public key K_{bd} of the data management center 33 to encrypt the received secret keys K_{sdi},

$C_{ksdikbd} = E\ (K_{bd},\ K_{sdi})$,

and broadcasts them by using a teletext broadcasting that utilizes the scan lines during the blanking intervals of analog television video signals; a data broadcasting that utilizes the subvoice-grade band of analog television audio signals; an FM multiplexed data broadcasting; or a digital data broadcasting. At this moment, the CATV broadcast station 31 may supply a non-encrypted table showing titles of available data for users' convenience of data usage or may supply a non-encrypted content guide describing the summaries of the data for the sake of promotion of data usage.

[0060] A user selects, from the table or from the content guide, data he or she desires to use, and then applies, by use of the data communication apparatus 35, for a data usage to the data management center 33 via the CATV line 37 and through the CATV broadcast station 31. At this moment, the user transmits his or her public key K_{bu} to the data management center 33. Having received the usage application from the user, the data management center 33 uses the corresponding secret key K_{sdi} to encrypt the data M,

$C_{mksdi} = E\ (K_{sdi},\ M)$,

and transmits it to the user terminal apparatus 38. At this moment, the private key K_{vd} of the data management center is encrypted by use of the public key K_{bu} of the user who has applied for the data usage,

$C_{kvdkbu} = E\ (K_{bu},\ K_{vd})$,

and then transmitted to the user terminal apparatus 38.

[0061] Having received the encrypted private key C_{kvdkbu} of the data management center, the user uses his or her private key K_{vu} to decrypt the encrypted private key C_{kvdkbu} of the data management center,

$K_{vd} = D\ (K_{vu},\ C_{kvdkbu})$,

and then uses the decrypted private key K_{vd} of the data management center to decrypt the encrypted secret key $C_{ksdikbd}$,

$K_{sdi} = D\ (K_{vd},\ C_{ksdikbd})$,

and then uses the decrypted secret key K_{sdi} of the data management center to decrypt the encrypted data C_{mksdi},

$M = D\ (K_{sdi},\ C_{mksdi})$,

and finally uses the data as decrypted.

Fourth Embodiment

[0062] The system structure of a fourth embodiment is the same as that of the third embodiment as illustrated in Fig. 4, and hence its description will not be repeated. Similarly to the third embodiment, the cryptographic key methods as employed in the present system are a secret key method and a public key method, but the fourth embodiment is different from the third one in the following points: in the third embodiment, the public key K_{bu} of the user, who applies for a data usage, is used to encrypt the private key K_{vd} of the data management center, which is then transmitted to the user, while in the fourth embodiment, the private key K_{vd} of the data management center is distributed, by use of an IC card or the like, and stored in the user terminal apparatus in advance; and further, in the third embodiment, data M is distributed in response to a data usage application, while in the fourth embodiment, data M is broadcasted via the CATV line or a satellite broadcasting independently of usage desire.

[0063] When a user enters into a comprehensive contract with the data management center to use the database thereof, the private key K_{vd} of the data management center, which is common to all the data to be supplied, is distributed to the user in advance via a recording medium, such as an IC card or the like, or via the CATV line 37, and stored into a semiconductor memory,

a hard disc device or a flexible disc in the user terminal apparatus 38. The data management center 33 prepares a public key K_{bd} as well as different secret keys K_{sdi} used for respective data to be supplied, and supplies them to the CATV broadcast station 31. Having received the secret keys K_{sdi}, the CATV broadcast station 31 uses the public key K_{bd} to encrypt them,

$C_{ksdikbd} = E\ (K_{bd},\ K_{sdi})$,

and broadcasts the encrypted secret keys $C_{ksdikbd}$ by using a teletext broadcasting that utilizes the scan lines during the blanking intervals of analog television vide signals; a data broadcasting that utilizes the subvoice-grade band of analog television audio signals; an FM multiplexed data broadcasting; or a digital data broadcasting. At this moment, the CATV broadcast station 31 may supply a non-encrypted table showing titles of available data for users' convenience of data usage or may supply a non-encrypted content guide describing the summaries of the data for the sake of promotion of data usage.

[0064] The CATV broadcast station 31 also uses the secret keys K_{sdi} to encrypt data M,

$C_{mksdi} = E\ (K_{sdi},\ M)$,

and unidirectionally broadcasts them via the CATV line independently of usage desires. The user uses the receiver apparatus 34 to capture, based on the table or the content guide, his desired data, from among the data being broadcasted via the CATV line, into the user terminal apparatus 38.

[0065] The use uses the private key K_{vd} of the data management center, which has been distributed and stored in advance into the semiconductor memory, hard disc device or flexible disc in the user terminal apparatus 38, to decrypt the encrypted secret key $C_{ksdikbd}$,

$K_{sdi} = D\ (K_{vd},\ C_{ksdikbd})$,

and then uses the decrypted secret key K_{sdi} to decrypt the encrypted data C_{mksdi},

$M = D\ (K_{sdi},\ C_{mksdi})$,

and finally uses the data as decrypted.

[0066] Other modified embodiments for distributing the

encrypted keys will be described below.

Fifth Embodiment

In each of the embodiments described above, the public key K_{bd} of the data management center is not transmitted via the communication line but broadcasted from the broadcast station, with the result that it is not possible to determine whether the public key is a true one. In such a case, the private key K_{vd} of the data management center is used to affix a digital signature to the public key K_{bd} of the data management center,

$S_{kbdkvd} = E\ (K_{vd},\ K_{bd})$,

and then the digital signature S_{kbdkvd} is broadcasted together with the public key K_{bd} of the data management center. The user uses the received public key K_{bd} of the data management center to ascertain the digital signature S_{kbdkvd},

$K_{bd} = D\ (K_{bd},\ S_{kbdkvd})$,

and uses the public key K_{bd} if it is the true one.

Sixth Embodiment

[0067] Further, if, in the fifth embodiment, the data management center employs a membership system in which usages of the database are registered in advance, then the public key K_{bui} of each user, who is a member, is registered with the data management center in advance. The data management center uses the public key K_{bui} of each user to encrypt the public key K_{bd} of the data management center,

$C_{kbdkbui} = E\ (K_{bui},\ K_{bd})$,

and further uses the private key K_{vd} of the data management center to affix the digital signature to the public key K_{bd} of the data management center,

$S_{kbdkvd} = E\ (K_{vd},\ K_{bd})$,

and then sends, to the broadcast station, the digital signature S_{kbdkvd} and each different encrypted public key $C_{kbdkbui}$ corresponding to the respective user. The broadcast station broadcasts each received encrypted public key $C_{kbdkbui}$ and digital signature S_{kbdkvd}. At this moment, as an occasion demands, non-encrypted user identification information of each user may be added to a respective encrypted public key $C_{kbdkbui}$ and then

broadcasted. Having received the broadcasted encrypted public key $C_{kbdkbui}$ and digital signature S_{kbdkvd}, a user uses his or her public key K_{bui} to decrypt the encrypted public key $C_{kbdkbui}$ of the data management center,

$K_{bd} = D\ (K_{bui},\ C_{kbdkbui})$,

and then stores the decrypted public key K_{bd} of the data management center into the user's terminal apparatus. Additionally, the user uses the received public key K_{bd} of the data management center to ascertain the digital signature S_{kbdkvd},

$K_{bd} = D\ (K_{bd},\ S_{kbdkvd})$,

and, if it is the true one, then uses the stored public key K_{bd} of the data management center. In this way, distribution of the different encrypted keys corresponding to the respective users can be achieved.

Seventh Embodiment

[0068] Each user presents his or her public key K_{bu} to the data management center each time he or she accesses or sends a request to the data management center. Having received the request from the user, the data management center uses the public key K_{bu} of the user to encrypt data M as requested,

$C_{mkbu} = E\ (K_{bu},\ M)$,

and sends it to the broadcast station, which then broadcasts the received encrypted data C_{mkbu}. Having received the broadcasted encrypted data C_{mkbu}, the user uses his or her private key K_{vu} to decrypt it,

$M = D\ (K_{vu},\ C_{mkbu})$,

and then uses the data M as decrypted.